PCT/ SE 00 / 0 1 8 4 2

SE00/1842

10/089548

4

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* *AB TryggIT, Borgholm SE*
Applicant (s)

(21) *Patentansökningsnummer* *9903575-0*
Patent application number

(86) *Ingivningsdatum* *1999-10-01*
Date of filing

Stockholm, 2000-10-31

För Patent- och registreringsverket
For the Patent- and Registration Office

A. Södervall

Anita Södervall

Avgift
Fee

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

AWAPATENT AB
Kontor/Handläggare
Göteborg/Fabian Johnsson/ANL

TRYGGVÄD AB
Ansökningsnr
Vår referens
SE-2006050

METOD OCH SYSTEM FÖR VERIFIERING AV TJÄNSTEBESTÄLLNING

Tekniskt område

Föreliggande uppfinning avser en metod och ett system för att verifiera uppdrag från en beställare till en tjänsteleverantör.

Teknisk bakgrund

Vid köp med kredit- eller betalkort i handeln finns ett ständigt problem att bestämma användarens identitet. Varje kort har vanligtvis en specifik kod, exempelvis en fyrställig sifferkod, vilken i vissa butiker kan matas in i samband med köpet. Detta är emellertid ingen speciellt attraktiv lösning för en person med ett tiotal kort, vardera med en specifik kod. I exempelvis restauranger tillämpas ofta systemet att gästen skriver under en bekräftelse av transaktionen, vilken underskrift fungerar som en efterkontroll om betalningen ifrågasätts. Detta innebär att kortets ägare endast i efterhand märker om någon använt kortet utan ägarens vetskap. Det förekommer till och med att restaurangens personal i bedrägligt syfte belastar ett kort med flera transaktioner under den tid de ensamma har tillgång till kortet. Ofta räcker det att en bedragare kommer över kortnumret, för att bedragaren sedan ska kunna använda detta kort vid ett senare tillfälle.

Enligt en känd teknik, avsedd för situationer där en kund har återkommande kontakt med exempelvis en bank, har kunden en skrapbar lista med koder. Banken har tillgång till samma lista, exempelvis lagrad i sitt datorsystem. Varje gång kunden beställer en transaktion, exempelvis via telefon, skrapar han fram ett nummer som anges. Numret kontrolleras mot bankens lista, varigenom säkerställs att kunden är den han utger sig för att vara, eller åtminstone har kommit över den aktuella skraplistan.

I kända system för säkra transaktioner på exempelvis Internet, förkommer en liten dosa, som användaren måste ha tillgång till vid transaktionstillfället. Genom att koder utväxlas mellan datorn och dosan säkerställs att användaren verkligen har tillgång till dosan, och transaktionen krypteras med en nyckel som beräknas av dosan och enbart används vid detta transaktionstillfälle. Denna teknik används framförallt i samband med banktjänster på Internet, då en användare relativt ofta utnyttjar tjänsten.

Lösningen med den personliga dosan uppvisar dock två problem:

För det första är det möjligt för en insatt fackman att kopiera elektroniken i en dosa som han har tillgång till en kort stund. Dosan kan sedan återlämnas till den intet ont anande ägaren. Ingen möjlighet finns sedan för datorsystemet att avgöra om det är ägaren eller bedragaren som beställer en transaktion.

För det andra är varje dosa specifik för varje tjänsteleverantör, vilket för en användare av flera tjänster innebär att ett flertal dosor ska medföras. Risken finns då att användaren har glömt den dosa som han för tillfället behöver. Vidare minskar användarens möjligheter att hålla samtliga dosor under uppsikt, och en bedragare kan lätt använda en stulen dosa, eller kopiera en "lånad" dosa, utan att användaren hinner sakna dosan.

När kontokort används för betalningar över Internet, är det oftast endast kontokortsnumret som fungerar som kontroll. Detta krypteras vanligen, men om krypteringen knäcks vid en transaktion av användarens namn tillsammans med kontokortsnumret, kan en bedragare handla relativt obehindrat tills användaren får en räkning, vanligtvis i slutet av månaden. Visserligen skulle dosor av ovan nämnt slag kunna utnyttjas för att förbättra säkerheten, men ovannämnda problem med kopiering av dosan, respektive behovet av flera dosor kvarstår då naturligtvis.

Vissa leverantörer har system på Internet där man först måste anmäla sig som kund, och först därefter kan handla med sitt kontokort. Dessa system har dock liksom dosan den nackdel att de är specifika för varje tjänsteleverantör, och användaren får därmed en mycket krånglig tillvaro i kontakten med flera olika leverantörer.

En annan mycket vanlig tjänst med behov av verifiering av användaren är inloggning i datorsystem, eller inpassering i säkerhetsklassade lokaler. Dessa system bygger nästan uteslutande på passerkort och på angivande av en kod eller ett lösenord, vilket i vissa system bytes enligt bestämda rutiner. Helt allmänt kan konstateras att det i vårt samhälle förekommer en uppsjö av koder, vilka för en människa är svåra att hålla i minnet. Frestelsen är därför stor att notera koderna någonstans, varvid säkerheten minskar.

Att kombinera angivandet av en kod med en dosa, vilken rent fysiskt måste finnas till hands förbättrar säkerheten, men till priset av en mängd dosor. Denna teknik är därför knappast någon universell lösning på ovanstående problematik.

Behov finns därför av ett enhetligt system som skulle kunna användas vid flera olika typer av tjänstebeställningar, genom vilket användarens legitimitet kan verifieras på ett enkelt sätt.

Definitioner

I den följande beskrivningen förekommer ett antal termer, vilka här definieras.

Med termen "uppdrag" avses helt allmänt en tjänst eller service som en person önskar utförd av en leverantör. Exempelvis kan ett uppdrag vara en ekonomisk transaktion, som utförs av en bank eller liknande, men ett uppdrag kan också vara en begäran att bli insläppt i en byggnad eller inloggad i ett datorsystem.

Med termen "tjänsteleverantör" avses både företaget som utför uppdraget (exempelvis en bank, ett kontokortfö-

retag eller ett säkerhetsbolag), och den utrustning som utför uppdraget (exempelvis ett portlås, en bankomat, eller ett datorsystem vid inloggning).

"Beställaren" är personen som begär uppdraget av tjänsteleverantören, och beställaren och tjänsteleverantören är i följande beskrivning tillika användare av metoden och systemet enligt uppfinningen.

Termen "databas" såväl den minnesenhet där data lagras som den mjukvara som hanterar datamängder och utför operationer exempelvis i syfte att jämföra datamängder.

Med "mobiltelefon" avses en bärbar telefon, exempelvis en GSM-telefon eller liknande. Även eventuella framtida bärbara telefoner innefattas naturligtvis av termen.

Uppfinningens syften

Ett första syfte med föreliggande uppfinning är att lösa ovanstående problem, och göra det möjligt att verifiera en beställare av en tjänst på ett tillfredsställande sätt.

Ett andra syfte med uppfinningen är att göra det möjligt att verifiera en beställare av en tjänst, vilken metod är universell, och enkelt kan utnyttjas av flera tjänsteleverantörer utan behov av för leverantören specifik utrustning.

Sammanfattning av uppfinningen

Dessa syften uppnås enligt uppfinning med en metod och ett system enligt de självständiga patentkraven 1, 13 och 14.

Enligt uppfinningen finns således för varje beställare två identiska uppsättningar kodord, av vilka den ena finns lagrad på en minneskrets i en mobiltelefon, och den andra finns lagrad i en databas. Verifikationen av beställaren utförs genom att mobilteleabonnemanget identifieras, ett kodord utvinns ur minneskretsen, och kodordet kontrolleras mot den kodordsuppsättning i databasen som direkt eller indirekt är associerad med mobilteleabonne-

manget. Den inbördes ordningen mellan ovannämnda moment kan naturligtvis vara annorlunda, såtillvida att kodordet kan utvinnas ur minneskretsen innan mobilteleabonnemanget identifieras.

En fördel med detta system i förhållande till känd teknik är att kodorden är av engångskaraktär i kombination med att ingen förutsägbar algoritm utnyttjas för att härleda nästa kodord. För att känna till kodorden i en uppsättning måste mobiltelefonens minneskrets stjälas rent fysiskt eller kopieras på exempelvis elektronisk väg.

Vidare är systemet användbart av ett obegränsat antal tjänsteleverantörer. Det enda som erfordras av tjänsteleverantören är utrustning för att koppla upp sig mot databasen och överföra kodordet och identiteten, och att motta resultatet av kontrollen. Detta innebär vidare att användaren genom att spärra sitt mobilteleabonnemang i databasen enkelt kan spärra samtliga tjänster som utnyttjar systemet.

En ytterligare fördel är att systemet är användbart helt parallellt med och oberoende av befintliga säkerhetssystem. Således kan varje tjänsteleverantör på egen hand välja om den vill ansluta sig till systemet, och därigenom förbättra säkerheten i sitt befintliga system.

Kodordet utvinns företrädesvis ur minneskretsen enligt en förutbestämd ordning, vilket ytterligare förbättrar verifikationens säkerhet. Förutom att kodordet kontrolleras tillhöra den kodordsuppsättning som är associerad med den uppgivna identiteten, kontrolleras också att det är rätt kodord inom uppsättningen.

I minneskretsen kan markeras när ett kodord har använts, och en liknande markering kan utföras i databasen. Härigenom säkerställs att minneskretsen och databasen har samma uppfattning om var i den förutbestämda ordningen nästa kodord ska hämtas. Man förhindrar alltså att minneskretsen och databasen kommer "ur fas". Detta system kan liknas vid att beställaren bär med sig en skrapbar

lista med kodord. För att använda ett kodord skrapas det fram, varvid tjänsteleverantören skrapar fram motsvarande kodord i sin lista och jämför de båda. För att beställningen ska accepteras måste rätt lista användas, och dessutom rätt kodord på listan.

En konsekvens av detta förfarande är att en bedragare som i lönndom kommit över en persons kodordsuppsättning, exempelvis genom att på elektronisk väg kopierat minneskretsen, endast kommer att kunna utnyttja minneskretsen om inte personen dessförinnan gjort en beställning, och därmed använt nästa kodord. Om bedragaren verkligen lyckas genomföra en beställning, kommer bedrägeriet att upptäckas senast nästa gång personen ska göra en beställning, eftersom det kodord som då anges inte accepteras. Mobilabonnemanget kan då spärras, varvid skadan minimeras. Jämför med en i lönndom kopierad säkerhetsdosa enligt känd teknik, som kan användas av en bedragare tills ägaren får ett uppseendeväckande kontouppdrag eller liknande.

Steget att identifiera mobilteleabonnemanget innefattar företrädesvis stegen att bestämma beställarens identitet, och att utifrån beställarens identitet identifiera mobilteleabonnemanget. Beställarens identitet kan utgöras av lämplig data, exempelvis ett personnummer, ett kontokortsnummer eller ett mobiltelefonnummer. Begreppet identitet betecknar egentligen enbart en direkt koppling till en person, och den data som representerar identiteten kan eventuellt utbytas. Sålunda kan identiteten från beställaren till tjänsteleverantören anges i form av exempelvis ett bank- eller passerskortsnummer med tillhörande kod, eller ett användar-ID med tillhörande kod, och från tjänsteleverantören till databasen anges i form av ett mobiltelefonnummer eller ett förutbestämt ID-nummer. Databasen måste dock kunna koppla ihop den mottagna identiteten med en bestämd kodordsuppsättning, normalt via mobiltelefonnumret, för att därigenom kunna kontrollera

att det angivna kodordet har utvunnits från rätt minneskrets.

Enligt en föredragen utföringsform skickas en begäran till beställaren att uppge ett kodord. Beställaren kan alltså beställa en tjänst på vanligt sätt, varpå tjänsteleverantören som en ytterligare säkerhetsåtgärd begär ett kodord, som beställaren då utvinner ur mobiltelefonen. Tjänsteleverantören har lämpligen information om vilka av dess kunder som är anslutna till systemet enligt uppfinningen, och skickar i förekommande fall en förfrågan till databasen. Databasen skickar därefter en begäran till beställaren att uppge ett kodord.

Begäran kan skickas via telenätet till mobiltelefonen och kodordet kan överförs från mobiltelefonen till databasen via telenätet. Lämpligen accepterar beställaren att kodordet skickas genom lämpliga knaptryckningar på mobiltelefonen. Eftersom härigenom två separata kommunikationsvågar utnyttjas, för det första en väg mellan tjänsteleverantören och databasen, och för det andra mellan databasen och mobiltelefonen, förbättras säkerheten ytterligare. En bedragare som uppfångat och förvanskat information längs den första kommunikationsvägen, har ingen möjlighet att förutse vilket mobilteleabonnemang eller basstation som nästa led i verifikationsprocessen kommer att utnyttja.

Begäran som skickas till mobiltelefonen, som exempelvis är ett SMS-meddelande eller liknande, kan innehålla information om transaktionen. Detta kan vara fördelaktigt exempelvis i en situation där kortet dragits i kortterminalen, och godkänts av kortföretaget, men där transaktionens belopp ännu inte fastställts. En bedragare skulle då, när hela verifikationen utförts, kunna ange ett felaktigt belopp, och därmed belasta beställarens konto för mycket. Genom ett SMS-meddelande enligt ovan skulle detta upptäckas av beställaren, som alltså får en slutlig bekräftelse till sin mobiltelefon.

Genom att mobiltelefonen kontaktas direkt ges en möjlighet för en användare att upptäcka ett pågående bedrägeri. Användaren kan då omedelbart spärra mobilabonnemanget, eller spärra det kort eller den tjänst som är utsatt för bedrägeri. Antag att någon stulit eller kopierat en persons kontokort, och dessutom lyckats komma över nästa kod på personens minneskrets. När kortet används, och en transaktion godkännes av databasen, skickas ett meddelande till mobiltelefonen, varpå innehavaren får kännedom om att någon använt en av koorden på minneskretsen. En möjlighet är vidare att dröja med kodordsbegäran till beställaren en bestämd tid. Detta skulle utesluta att en bedragare använder en mobiltelefon som sedan lämnas tillbaka, utan att ägaren märker det. Fördröjningstiden kan anpassas så att mobiltelefonens ägare hinner sakna den och spärra den innan begäran om kodord skickas till mobiltelefonen och därmed verifierar beställningen.

Samtidigt möjliggör denna metod att en beställare kan låta en tredje person använda beställarens kort för en bestämd tjänst, exempelvis att köpa en vara. Beställaren får oavsett var han befinner sig, en bekräftelse på att köpet stämmer, och gör den definitiva bekräftelsen via sin mobiltelefon.

Speciellt vid tjänstebeställningar via Internet är det fördelaktigt med en begäran från databasen eller tjänsteleverantören direkt till mobiltelefonen, eftersom all information som överförs via Internet är mer eller mindre åtkomlig för andra. Ett SMS-meddelande till beställarens telefon blir därför en utmärkt kvittens på att transaktionen är korrekt.

Enligt en annan utföringsform av uppfinningen överförs beställarens identitet och det ur minneskretsen utvunna kodordet till tjänsteleverantören, mobilteleabonnemanget som är associerat till beställaren identifieras av tjänsteleverantören, och kodordet och mobilteleabonnemangets identitet överförs till databasen av tjänsteleverantören. Med detta förfarande kan beställaren alltså di-

rekt i samband med beställningen överföra både sin identitet och ett kodord till tjänsteleverantören. Identifieringen av mobilteleabonnemanget utförs därefter antingen av tjänsteleverantören eller av databasen.

Enligt en ytterligare utföringsform av uppfinningen utvinns ett andra kodord från minneskretsen och överförs till databasen, för att ytterligare verifiera uppdraget. Kodorden i uppsättningen kan vara associerade till varandra i grupper med olika antal kodord, för att användas vid olika typer av tjänstebeställningar med olika säkerhetsnivå.

Det första kodordet kan överföras från beställaren till databasen, eventuellt via tjänsteleverantören, varpå databasen skickar en begäran till beställaren att uppge ett andra kodord, och slutligen det andra kodordet överförs från beställaren till databasen. Begäran till beställaren kan ske på samma sätt som den ovan beskrivna begäran. En möjlighet är alltså att beställaren direkt till mobiltelefonen, får två på varandra följande begäran om att överföra ett kodord. En annan möjlighet är att beställaren först anger ett kodord direkt i samband med beställningen, varpå beställaren därefter får en begäran om att ange ett ytterligare kodord. Fler möjligheter är naturligtvis möjliga, och speciellt kan även mobiltelefonens PIN-kod utnyttjas som ett sätt att ytterligare höja säkerheten i verifikationen.

Enligt en utföringsform av uppfinningen lagras i databasen även positionsangivelser som är associerade med mobilteleabonnemanget. Vid verifikationen lokaliseras minneskretsen, och den erhållna positionen kan jämföras med de i databasen lagrade positionsangivelserna. Detta förfarande kan utnyttjas för att geografiskt begränsa var en beställare kan utföra vissa typer av tjänster. Exempelvis kan köp över ett visst belopp vara begränsade till ett fåtal, förutbestämda platser, vilket ytterligare ökar säkerheten. Denna geografiska kontroll kan också vara tillämpbart vid inloggning i ett datorsystem, som kanske

endast är tillåten från arbetsplatsen eller hemifrån. Alternativt kan en positionsangivelse i databasen vara en IP-adress, varigenom inloggningsförfarande eller Internettransaktioner kan begränsas till en bestämd dator, utan att denna information finns tillgänglig hos tjänsteleverantören eller någonstans på Internet.

Kort beskrivning av ritningarna

Föreliggande uppfinning kommer i det följande att beskrivas närmare under hänvisning till bifogade ritningar, vilka i exemplifierande syfte visar föredragna utföringsformer av uppfinningen.

Fig 1a-b visar två kodordsuppsättningar enligt uppfinningen.

Fig 2 visar en mobiltelefon enligt uppfinningen.

Fig 3 visar en databas enligt uppfinningen.

Fig 4 visar hur kodordsuppsättningar enligt fig 1 framtages och lagras.

Fig 5a-d visar fyra föredragna utföringsformer av metoden enligt uppfinningen.

Beskrivning av en föredragen utföringsform

I fig 1a-b visas två exempel på en kodordsuppsättning 1, som består av ett flertal koder 2 i form av fyr- eller sexställiga sifferkombinationer. Dessa sifferkombinationer är helt slumpmässigt framtagna, och uppvisar inget härledbart samband, vare sig avseende sammansättning eller ordningsföljd. Koderna kan vara ordnade i grupper 3, med två eller flera koder 2 i varje grupp.

Eftersom varje kod i sig är helt oberoende av de övriga finns inget hinder mot att en sifferkombination förekommer flera gånger i samma uppsättning, eller till och med i samma grupp.

Kodordsuppsättningen 1 är associerad med en identitet 4, som direkt eller indirekt är förknippad med ett mobiltelеabonnemang. I det visade exemplet utgörs identiteten av ett mobiltelefonnummer 5.

Mobiltelefonen 10 som schematiskt visas i fig 2 har på känt vis en knappsats 11, en display 12, samt en mottagare/sändare 13. Mobiltelefonen har vidare en minneskrets 15, exempelvis ett SIM-kort eller motsvarande smart-card, vilken innehåller information 16 om mobiltelefonabonnemanget. Exempelvis kan ett SIM-kort innehålla information om abonnemangets telefonnummer, och om hur mycket kredit som återstår på ägarens konto hos mobiltjänstleverantören. Minneskretsen 15 är vidare enligt uppfinningen försedd med den kodordsuppsättning 17 som är associerad med abonnemanget.

SIM-kortet kan förses med ett abonnemangs-ID och en kodordsuppsättning innan det levereras till en återförsäljare under noggrann sekretess, exempelvis genom någon form av sigillförslutning. Användaren som köper eller på annat sätt kommer över SIM-kortet kontrollerar att sigillet inte är brutet och anordnar därefter SIM-kortet i sin mobiltelefon för att kunna använda denna.

Den i fig 2 visade mobiltelefonen är vidare försedd med organ, exempelvis en mjukvara 18, för att från minneskretsen 15 utvinna ett kodord från kodordsuppsättningen 17, och sända detta medelst mobiltelekombination, exempelvis i ett SMS-meddelande. En mjukvara med denna funktionalitet kan utvecklas av en fackman på området. Mjukvaran 18 kan också överföra ett kodord via en kommunikationsport 19, såsom en seriell eller parallell dataöverföringsport, eller infraröd port. Vidare kan ett utvunnet kodord visas på displayen 12.

Mjukvaran 18 är vidare anordnad att motta ett kodord och jämföra kodordet med kodordsuppsättningen i minneskretsen. Kodordet kan inmatas medelst knappsatsen 11, eller också mottas medelst mobiltelekommunikation direkt till mobiltelefonens mottagare 13, exempelvis genom att mobiltelefonen mottar ett SMS-meddelande.

Det är lämpligt att mobiltelefonen kan försättas i ett sov-läge, där inga telefonsamtal tas emot, men där

SMS-meddelanden kan mottas och sändas. Denna funktion kan utvecklas av en fackman på området.

I databasen 21, som visas i fig 3, är ett flertal kodordsuppsättningar 22 lagrade, vilka vardera har en identitet 23 som är associerad till ett mobilteleabonnemang, vars motsvarande SIM-kort innefattar en identisk kodordsuppsättning.

Varje uppsättning 22 kan vidare vara kopplad till en eller flera positionsangivelser 24. Positionsangivelserna kan exempelvis vara ställen på vilka beställaren angivit att han vill kunna utföra en viss typ av beställningar.

Databasen 21 är vidare försedd med kommunikationsorgan 25 för att motta en förfrågan, samt meddela resultatet av verifikationen. Exempelvis kan kommunikationsorganet 25 utgöras av ett modem som är anordnat att kommunicera med tjänsteleverantören, till exempel att motta ett kodord och en identitet från tjänsteleverantören, samt att skicka en bekräftelse till tjänsteleverantören om att uppdraget är verifierat. Kommunikationsorganet 25 kan också vara anordnat att över mobiltelenätet, exempelvis via SMS-meddelanden, kommunicera med mobiltelefonen.

Vidare är databasen 21 försedd med organ, företrädesvis mjukvara 26, som är anordnad att utföra sökningar i databasen och att exempelvis verifiera att ett bestämt kodord återfinns i den kodordsuppsättning 22 i databasen som är associerad en bestämd identitet 23.

I fig 4 illustreras hur kodordsuppsättningar 1 bildas och lagras.

I ett helt fristående datorsystem slumpas sifferkombinationer fram enligt algoritmer som inte kan förutsägas utifrån (steg 31). Detta säkerställer att ingen kan förutse vilka kodord som ingår i en bestämd kodordsuppsättning, och kan enkelt åstadkommas av en fackman på området. Sifferkombinationerna grupperas i grupper och uppsättningar (steg 32), enligt algoritmer som i sig kan tillåtas vara kända utanför datorsystemet. Datorsystemet tillförs vidare en serie mobiltelefonnummer, vilka till-

handahålls av en mobilteletjänstleverantör, och associerar varje kodordsuppsättning med ett telefonnummer (steg 33).

Därefter distribueras uppsättningarna (steg 34) till företag som förser SIM-korten med information, där varje kodordsuppsättning lagras på ett SIM-kort (steg 35) som antingen före eller efter lagringen har tilldelats det mobiltelenummer som uppsättningen är associerad till.

Vidare distribueras (steg 34) uppsättningarna till databasen, där de också lagras (steg 36). Uppsättningarna kan lagras på åtkomstskyddade informationsbärare, exempelvis kodade och sigillförslutna CD-skivor, vilka distribueras på säkert sätt, exempelvis med kurir. Om datorsystemet som bildar uppsättningarna är anslutet till databasen, kan denna del av distributionen ske på säker elektronisk väg.

I fig 5a - c illustreras översiktligt tre olika varianter av hur verifikationen av ett uppdrag från en beställare 41 till en tjänsteleverantör 42 går till enligt uppfinningen. I samtliga fall har beställaren 41 en mobiltelefon 10 enligt fig 2.

Enligt metoden i fig 5a uppger beställaren först sin identitet 43 till tjänsteleverantören 42. Detta sker normalt i samband med beställningen av uppdraget, då beställaren exempelvis uppger ett användar-ID, ett kontokortsnummer eller annan information som för tjänsteleverantören identifierar beställaren.

Tjänsteleverantören har kännedom om vilka kunder som är anslutna till systemet enligt uppfinningen, och har möjlighet att associera ett mobilteleabonnemang till kundens identitet. Tjänsteleverantören 42 skickar en förfrågan 44 till databasen 21, och överför mobilteleabonnemangets identitet 23, vanligen i form av ett mobiltelenummer, men eventuellt i form av ett annan identifikation som är associerad med mobilteleabonnemanget, till databasen 21. Naturligtvis kan istället beställarens identitet

43 överföras till databasen 21, och det aktuella mobiltelefonabonnemanget identifieras av databasen.

Databasen skickar därefter en begäran 45 via telenätet till mobiltelefonen 10, exempelvis medelst ett SMS-meddelande eller liknande. Meddelandet 45 innehåller information om beställningen, som visas i displayen 12, så att beställaren kan kontrollera att beställningen är riktig. Om så är fallet kan beställaren bekräfta på lämpligt sätt, exempelvis med en dubbel knapptryckning på bestämd knapp i knapsatsen 11. Exempelvis kan beställaren till sin mobiltelefon få ett meddelande av typen "Kortköp $35 på BurgerKing. Tryck OK för att bekräfta", eller "Du loggar nu in på din arbetsplats. Tryck OK för att bekräfta". Beställaren trycker då på OK-knappen. En ytterligare bekräftelse av typen "Är du säker J/N" kan vara lämplig, som en extra kontroll. Mjukvaran 18 i mobiltelefonen hämtar då från SIM-kortet 15 nästa, ännu inte använda kod 46, och skickar denna från mobiltelefonen 10 till databasen 21. Samtidigt markeras det skickade kodordet som använt på SIM-kortet. Begäran 45 från databasen kan också innehålla ett kodord (ej visat), som av mobiltelefonens mjukvara 18 kontrolleras mot SIM-kortets 15 kodordsuppsättning 17.

En annan möjlighet är att databasen 21 kontaktar tjänsteleverantören 42, som i sin tur begär ett kodord från beställaren och returnerar detta till databasen 21.

När databasen 21 får kodordet 46 kan det jämföras med den uppsättning 22 som är associerad till mobiltelefonabonnemanget. Om kontrollen misslyckas, exempelvis berorende på att koden inte återfinns i kodordsuppsättningen i databasen som är associerad till telefonnumret, överförs information om detta till tjänsteleverantören, som kan vägra utföra tjänsten, exempelvis vägra tillträde till ett datorsystem eller stoppa en transaktion. Om kontrollen däremot är positiv, dvs den angivna koden är korrekt, överförs ett klartecken 47 till tjänsteleverantören 42,

som då kan utföra tjänsten. Samtidigt markeras det mottagna kodordet som använt.

Enligt metoden som visas i fig 5b uppger beställaren 41 ett kodord 46 i samband med att beställaren uppger sin identitet 43 enligt ovan. Beställaren 41 kan exempelvis läsa av ett kodord 46 från mobiltelefonens 10 display 12, och överföra det till tjänsteleverantören 42. Alternativt kan en dataöverföringsport 19 hos mobiltelefonen användas för att överföra ett kodord till tjänsteleverantören.

Tjänsteleverantören skickar därefter en förfrågan 44 till databasen 21, och överför förutom identiteten enligt ovan, även kodordet 46. Databasen 21 kontrollerar kodordet enligt ovan, och skickar ett klartecken 47 till tjänsteleverantören 42.

Metoden som visas i fig 5c är egentligen en kombination av de två tidigare metoderna. Beställaren 41 uppger först ett kodord 46' i samband med beställningen enligt fig 5b, och mottar därefter en begäran 45 om ytterligare ett kodord 46'' enligt fig 5a.

För att ytterligare öka säkerheten kan mjukvaran 18 vara anordnad att vid vissa uppdrag, exempelvis köp över ett visst belopp, begära användaren PIN-kod för att utvinna och sända kodordet. Detta innebär att en bedragare som kommit över en påslagen mobiltelefon ändå är tvungen att känna till ägarens PIN-kod.

De i databasen lagrade positionsangivelserna kan också utnyttjas för att höja säkerheten. Den basstation som mobiltelefonen kommunicerar via kan relativt enkelt identifieras, och en jämförelse med de lagrade positionsangivelserna kan utföras. Det kan också vara möjligt att i mobiltelefonen innefatta en GPS-navigator eller liknande, varvid mobiltelefonen kan kommunicera sin position mycket noggrant. Positionskontrollen skulle härvid kunna ske i två steg, först grovt, med avseende på basstation, och sedan mer noggrant, med avseende på longitud och latitud.

Ytterligare varianter och kombinationer av dessa metoder kan förekomma inom ramen för uppfinningen. Antalet kodord som utbyts mellan mobiltelefonen och databasen kan variera beroende på den önskade säkerheten.

I det följande ges några exempel på situationer då en verifikationsmetod enligt uppfinningen är speciellt lämplig.

Restaurang

En gäst som åtit på en restaurang beställer av sitt kontokortsföretag eller liknande tjänsten att betala restaurangnotan med medel som finns på gästens eget konto eller på kontokortsföretagets konto (kreditkort). Kortföretaget är således tjänsteleverantör, och gästen är beställare.

På känt vis hanteras kontokortet av restaurangpersonalen, för att verifiera kortets nummer, dess giltighet, att medel finns på kontot, att kortet inte är spärrat etc. Kortföretaget får på detta sätt kännedom om beställarens identitet, exempelvis genom det unika kortnumret. Enligt en vanligt förekommande teknik dras kortet i en kortterminal, som via modem kontaktar kortföretaget och kontrollerar transaktionen.

Kortföretaget har i ett register information om att beställaren är ansluten till systemet enligt uppfinningen, och identifierar mobilteleabonnemangets telefonnummer. Detta skickas till databasen, vilken därefter kontaktar mobiltelefonen via telenätet och mottar ett kodord (fig 5a).

Alternativt använder beställaren sin mobiltelefon för att i samband med beställningen uppge ett kodord (fig 5b). Kodordet kan överlämnas till restaurangpersonalen, som via kortterminalen åter kontaktar kortföretaget och överför koden, eller också överföras från mobiltelefonen till kortterminalen genom någon form av kommunikationsorgan, exempelvis en IR-port.

När kodordet verifierats av kortföretaget skickas ett klartecken 47 till restaurangen, varvid ett kvitto skrivs ut.

Internettransaktion

Förfarandet är snarlikt när en datoranvändare vill göra en transaktion på Internet eller liknande, exempelvis göra en girering från ett av sina bankkonton, eller handla med ett kontokort. Datoranvändaren är då beställare av en tjänst i form av en transaktion. Tjänsteleverantören kan vara ett kortföretag enligt ovan eller beställarens egen bank.

Beställarens identitet överförs i detta fall genom en inmatning av exempelvis ett personnummer och tillhörande lösenord eller ett kontokortsnummer eller liknande. En sådan inmatning kan ske i en skärmbild på en WWW-sida, varefter sidans innehåll med en knapptryckning skickas till sidans innehavare.

Om ett förfarande enligt fig 5a används blir förloppet identiskt med det ovan beskrivna exemplet, och beställaren får inom någon minut ett SMS-meddelande till sin mobiltelefon, och kan bekräfta beställningen genom lämpliga knapptryckningar. Om ett förfarande enligt fig 5b utnyttjas, där beställaren låser av ett kodord från mobiltelefonens display, kan kodordet överföras på samma sätt som identiteten, antingen på samma WWW-sida eller vid en efterföljande sida, som dyker upp så snart identiteten godkänts.

Inloggning/inpassering

Ytterligare en tjänstekategori som lämpar sig för verifikation enligt uppfinningen är inloggning i ett datorsystem. Beställaren är då personen som vill åtkomma systemet, tjänsten är att släppa in personen i datorsystemet eller liknande, och tjänsteleverantören är det företag eller datorsystem som är ansvarigt för säkerheten.

Beställaren anger sin identitet vid en inloggning enligt känd teknik, och uppger därvid exempelvis ett användar-ID med lösenord. Därefter kan tjänsteleverantören

kontakta databasen som begär ett kodord direkt från mobiltelefonen enligt fig 5a. Alternativt kan beställaren enligt fig 5b ges möjlighet att via tangentbordet ange en kod som avlästs ur mobiltelefonens display.

Vid fysisk inpassering till en lokal eller ett område blir situationen snarlik den vid inloggning. Exempelvis kan då beställarens identitet anges genom att dra ett passerskort eller slå en kod på ett portlås.

Exempel på detaljerad händelsekedja vid betalning på en restaurang, i en affär etc.

Nedan görs, med hänvisning till fig 5d, en mer detaljerad beskrivning av en tänkbar kedja av händelser för att en legitim beställare skall kunna utföra ett uppdrag med mycket hög säkerhet. Om uppdraget inte har så hög säkerhetsklassning kan vissa moment uteslutas ur händelsekedjan. Det är lämpligen tjänsteleverantörens dator som avgör vilken säkerhetsklass som uppdraget skall ha och om dricks ska lämnas till försäljningsstället. Därmed styrs resten av händelsekedjan baserat på säkerhetsklass och om dricks ska lämnas eller ej.

a) Beställaren 41 lämnar ifrån sig ett kreditkort 51.

b) Kreditkortet dras i kortterminalen 52 och betalningsbeloppet (inklusive eventuella garderobsavgifter mm) matas in i terminalen. Terminalen 52 genererar ett meddelande om önskad betalning som bl.a. innehåller kortnummer, kortterminalens nummer och betalningsbeloppet.

c) Kortterminalen skickar det i (b) genererade meddelandet till kreditkortföretagets dator (tjänsteleverantören 42).

d) Kreditkortföretagets dator kreditprövar transaktionen och om denna prövning faller väl ut så genererar datorn ett meddelande om transaktionen (säljare och belopp mm), uppdragsnummer, uppdragets säkerhetsklass, om "dricks" förekommer samt kreditkortinnehavarens mobiltelefonnummer.

e) Kreditkortföretagets dator skickar det meddelande som genererats i (d) till databasen 21.

f) Databasen 21 plockar fram nästa oanvända kodord, kollar med aktuell mobiloperatör 54 om mobilen är på en tillåten plats och genererar ett meddelande med begäran om bekräftelse av uppdraget. I meddelandet ingår bl.a. säljare, belopp, uppdragsnummer, säkerhetsklass, om dricks förväntas och nästa oförbrukade kodord (576362).

g) Databasen 21 skickar det meddelande som genererats i (f) till beställarens mobil 10.

h) Mobilen kollar vilken säkerhetsklass som gäller och om dricks förekommer. Baserat på detta väljer mobilen vilken rutin som skall verkställas. Mobilen lägger upp förfrågan på displayen och ber om bekräftelse. Beställaren trycker på bekräfta. Om det är en hög säkerhetsklass begär mobilen att beställaren trycker in PIN-koden eller ett motsvarande lösenord som bara beställaren har i sitt huvud. Om det är ett säljställe (exempelvis restaurant) som tillämpar dricks, kommer det en fråga på mobilens display om beloppet skall höjas och då kan beställaren mata in ett nytt högre belopp. Mobilen ber beställaren att åter bekräfta och om beställaren på nytt bekräftar så genereras antingen ett eller två meddelanden beroende på säkerhetsklass. Båda meddelandena innehåller bl.a. mobiltelefonnummer, uppdragsnummer, säljare, belopp, slutligt belopp (om dricks) det första oförbrukade kodordet (576362) och nästa oförbrukade kodord (805209) och om mobiltelefonen har inbyggd GPS-mottagare så bifogas även GPS-koordinaterna. Mobilen noterar de båda kodorden som förbrukade. Hela detta steg (h) hanteras av mjukvaran 18 i mobiltelefonen 10, vilken kan utvecklas av en fackman på området.

i) Mobilen 10 sänder det i (h) genererade meddelandet till databasen 21.

j) Mobilen 10 sänder det i (h) genererade meddelandet till kreditkortföretagets dator 42.

k) Databasen 21 kontrollerar meddelandet från mobilen och om båda kodorden är korrekta genereras ett ID-bekräftelsemeddelande i vilket bl.a de båda kodorden ingår och de båda kodorden noteras som förbrukade.

l) Databasen 10 sänder det i (k) genererade ID-bekräftelsemeddelandet till kreditkortföretagets dator 42.

m) Kreditkortföretagets dator kontrollerar meddelandet från mobilen (j) och ID-bekräftelsemeddelandet från databasen (l) och gör lämpliga jämförelser. Om allt faller väl ut så genereras en skrivorder som innehåller lämpliga uppgifter exempelvis säljare, köpare, belopp, kreditkortsnummer, uppdragsnummer, datum, klocka och verifikationsnummer.

n) Skrivorden överföres till kortterminalen 52.

o) Kortterminalen skriver ut transaktionskvittot 53.

p) Beställaren får tillbaka kreditkortet 51 och skriver under transaktionskvittot 53 och tar kopian medan säljaren behåller originalet.

Följande är vad beställaren upplever av ovanstående händelsekedja.

- Beställaren lämnar sitt kreditkort som vanligt.
- Beställaren får upp betalningen på sin mobiltelefondisplay inom någon minut och bekräftar uppdraget genom två knapptryckningar. Vid stora uppdrag (hög säkerhetsklass) får beställaren mellan den första och andra bekräftelsen, mata in PIN-koden eller annat liknande lösenord och eventuellt justerar upp beloppet, d.v.s. ger dricks.
- Beställaren får skriva under transaktionskvittot och ta kopian som vanligt.

Tillkommande moment: Beställaren bekräftar genom två knapptryckningar betalningen plus matar eventuellt in PIN-kod och höjer beloppet om dricks ska ges.

Moment som försvinner: Beställaren slipper att visa legitimation.

Följande är vad säljaren upplever av ovanstående händelsekedja.

- Säljaren tar kreditkortet och drar detta genom kortterminalens låsare som vanligt.
- Säljaren matar in beloppet via kortterminalen som vanligt.
- Säljaren river av transaktionskvittot som vanligt.
- Säljaren tillser att beställaren skriver under transaktionskvittot och tar originalet som vanligt.

Tillkommande moment: Inga

Moment som försvinner: Säljare slipper begära legitimation, kontrollera legitimation och skriva legitimationsnummer.

<u>Tänkbara varianter på ställen där betalningen måste ske snabbt</u>

Man kan exempelvis vid betalning av mindre belopp i affär, kiosk, bensinstation mm tänka sig att bekräftelsen inte sker över mobilnätet, eftersom detta kan ta någon minut extra. Istället kan exempelvis mobiltelefonens infraröda dataöverföringsport 19 användas. I detta fall utrustas också kortterminalen med en infraröd kanal (ej visad) och programvara, samt en display om inte kassaapparaten redan har en display riktad mot kundsidan. Den infraröda enheten sitter lämpligen i displayenheten eller nära denna.

För denna utförandeform drar säljaren beställarens kreditkort och matar in beloppet eller får det direktöverfört från exempelvis den bensinpump som beställaren just använt d.v.s. som det fungerar idag. När detta är klart visas beloppet på ovan nämnda display, vilken också uppmanar beställaren att exempelvis "Bekräfta betalningen med din mobil". Beställaren riktar sin mobil mot display-

en och mottar exempelvis bensinstationens namn och det aktuella beloppet. Genom två bekräftelsetryckningar på mobilen så överföres det första oanvända kodordet till kortterminalen och displayen kan exempelvis visa "Lösenord mottagits". Därefter fungerar allt som idag.

Man kan säga att mobilen ersätter den kontrollknappsats som är vanlig på många bensinstationer i åtminstone Sverige. Någon som står bredvid kan emellertid se vilken kod som slås in även om det finns ett skydd som skall göra det svårare att se. Om den som just slog in sin kontrollkod skulle glömma sitt kort på disken föreligger en frestelse för en oärlig person. En sådan person skulle kunna lägga handen över den förra kundens kreditkort och låta det glida ner i fickan. Den oärlige personen skulle sedan kunna tanka upp exempelvis familjens bilar innan kortets riktiga ägare någon vecka senare skall tanka sin bil på nytt och märker att kreditkortet är borta.

Uppfinningen innebär ju att ett kodord aldrig används mer än en gång och för övrigt är det normalt ingen, varken beställaren eller annan, som ser några kodord över huvud taget.

Avslutning

Det inses att en mängd varianter av de ovan beskrivna utföringsformerna är möjliga inom ramen för de bifogade patentkraven. Exempelvis kan ett stort antal alternativa verifikationsförfarande genomföras med ett system enligt uppfinningen. På samma sätt kan annorlunda utrustning än den här beskrivna användas för att verkställa metoden enligt uppfinningen.

PATENTKRAV

1. Metod att verifiera uppdrag från en beställare (41) till en tjänsteleverantör (42), innefattande stegen

att bilda ett flertal uppsättningar (1) slumpmässigt framtagna kodord (2),

att lagra en av nämnda flertal kodordsuppsättningar (1) i en till ett mobilteleabonnemang associerad minneskrets (15) i en mobiltelefon (10),

att lagra en identisk kodordsuppsättning (1) i en databas (21) tillsammans med en association till nämnda mobilteleabonnemang, och

att vid beställningstillfället identifiera nämnda mobilteleabonnemang, utvinna åtminstone ett kodord (46) ur minneskretsen och kontrollera att kodordet förekommer i den kodordsuppsättning (1) i databasen som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

2. Metod enligt krav 1, varvid kodordet utvinns från minneskretsen (15) enligt en förutbestämd ordning, vilken ordning är känd av databasen.

3. Metod enligt krav 2, vidare innefattande steget att i åtminstone den ena av minneskretsen (15) och databasen (21) markera när ett kodord (46) har använts, varigenom säkerställs att nämnda förutbestämda ordning följs.

4. Metod enligt något av föregående krav, varvid steget att identifiera mobilteleabonnemanget innefattar stegen

att bestämma beställarens identitet, och

att utifrån beställarens identitet identifiera mobilteleabonnemanget.

5. Metod enligt något av föregående krav, varvid en begäran (45) att uppge ett kodord skickas till beställaren.

6. Metod enligt krav 5, varvid begäran (45) skickas till mobiltelefonen (10) via telenätet.

7. Metod enligt krav 5 eller 6, varvid kodordet överförs från mobiltelefonen (10) till databasen (21) via telenätet.

8. Metod enligt krav 1 - 3, varvid beställarens identitet (43) och det ur minneskretsen utvunna kodordet (46) överförs till tjänsteleverantören (42),. mobilteleabonnemanget som är associerat till beställaren identifieras av tjänsteleverantören, och kodordet (46) och mobilteleabonnemangets identitet (23) överförs till databasen av tjänsteleverantören.

9. Metod enligt något av föregående krav, varvid ett andra kodord (46'') utvinns från minneskretsen (15) och överförs till databasen (21), för att ytterligare verifiera uppdraget.

10. Metod enligt krav 9, varvid kodorden i uppsättningen är associerade till varandra i grupper (3), och nämnda första (46') och andra (46'') kodord ingår i samma grupp kodord.

11. Metod enligt krav 9 - 10, varvid nämnda första kodord (46') överförs från beställaren (41) till databasen (21), databasen skickar en begäran (45) till beställaren att uppge nämnda andra kodord (46''), varvid nämnda andra kodord överförs från beställaren till databasen (21).

12. Metod enligt något av föregående krav, vidare innefattande stegen

att till mobilteleabonnemanget associera och i databasen (21) lagra åtminstone en positionsangivelse (24),

att vid varje beställningstillfälle bestämma var minneskretsen (15) är lokaliserad, och kontrollera den sålunda erhållna positionsangivelsen med nämnda, i databasen lagrade positionsangivelse (24).

13. Metod att verifiera ett uppdrag från en beställare till en tjänsteleverantör, varvid en uppsättning (1) slumpmässigt framtagna kodord (2) har lagrats i en till ett mobilteleabonnemang associerad minneskrets (15) i en mobiltelefon (10) samt i en databas (21) tillsammans med en association (23) till nämnda mobilteleabonnemang, innefattande stegen

att bestämma beställarens identitet (43),

utifrån beställarens identitet identifiera mobilteleabonnemanget,

att utvinna ett kodord (46) ur minneskretsen, och

att kontrollera att nämnda kodord förekommer i den kodordsuppsättning (22) i databasen (21) som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

14. System för verifiering av ett uppdrag från en beställare (41) till en tjänsteleverantör (42), innefattande

en mobiltelefon (10) med en till ett mobilteleabonnemang associerad minneskrets (15),

organ för att låta beställaren till tjänsteleverantören uppge sin identitet (43),

kännetecknat av att systemet vidare innefattar

en databas (21),

en uppsättning (1) slumpmässigt framtagna kodord (2), vilken uppsättning för det första är lagrad i minneskretsen (15), och för det andra är lagrad i databasen

(21) och där är förknippad med mobilteleabonnemanget,

organ för att utifrån beställarens identitet (43) identifiera mobilteleabonnemanget,

organ för att låta beställaren (41) utvinna ett kodord ur minneskretsen (15), och överföra nämnda kodord till databasen (21), och

kontrollorgan (25, 26) för kontrollera att nämnda kodord förekommer i den kodordsuppsättning (22) i databasen som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

15. System enligt krav 14, varvid kontrollorganet innefattar ett kommunikationsorgan (25) för att kommunicera mellan databasen (21) och mobiltelefonen (10).

SAMMANDRAG

Uppfinningen avser en metod och ett system för att verifiera ett uppdrag från en beställare (41) till en tjänsteleverantör (42), varvid en uppsättning slumpmässigt framtagna kodord har lagrats i en till ett mobilteleabonnemang associerad minneskrets i en mobiltelefon (10) samt i en databas (21) tillsammans med en association till nämnda mobilteleabonnemang. Metoden innefattar stegen att bestämma beställarens identitet (43), att utifrån beställarens identitet identifiera mobilteleabonnemanget, att utvinna ett kodord (46) ur minneskretsen, och att kontrollera att nämnda kodord förekommer i den kodordsuppsättning i databasen (21) som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

Publ. bild = fig 5a

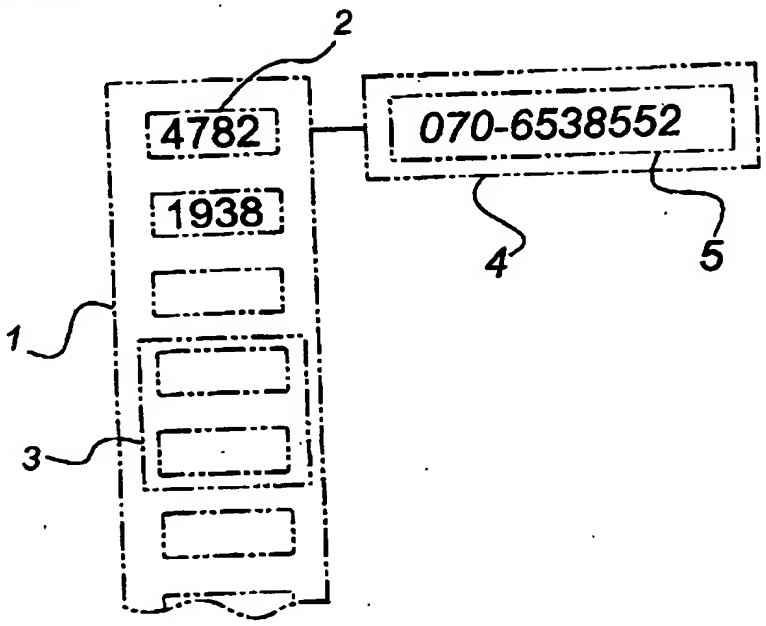

Fig 1a

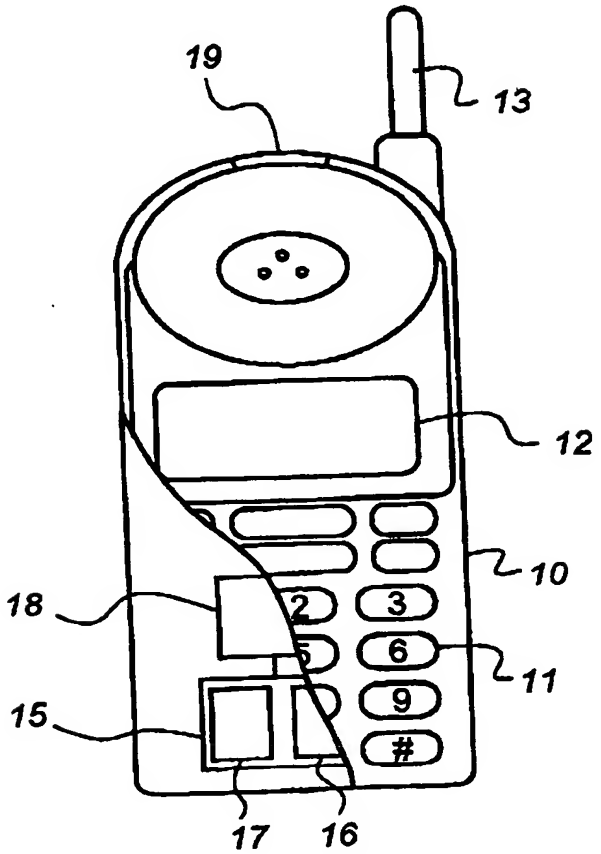

Fig 2

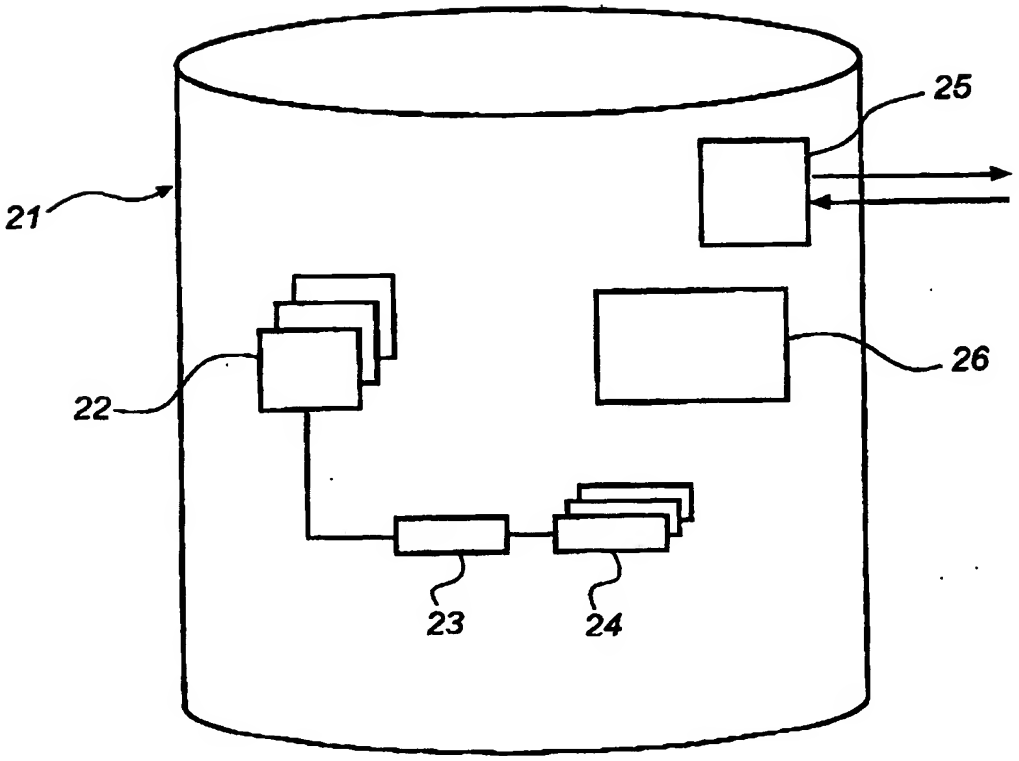

Fig 3

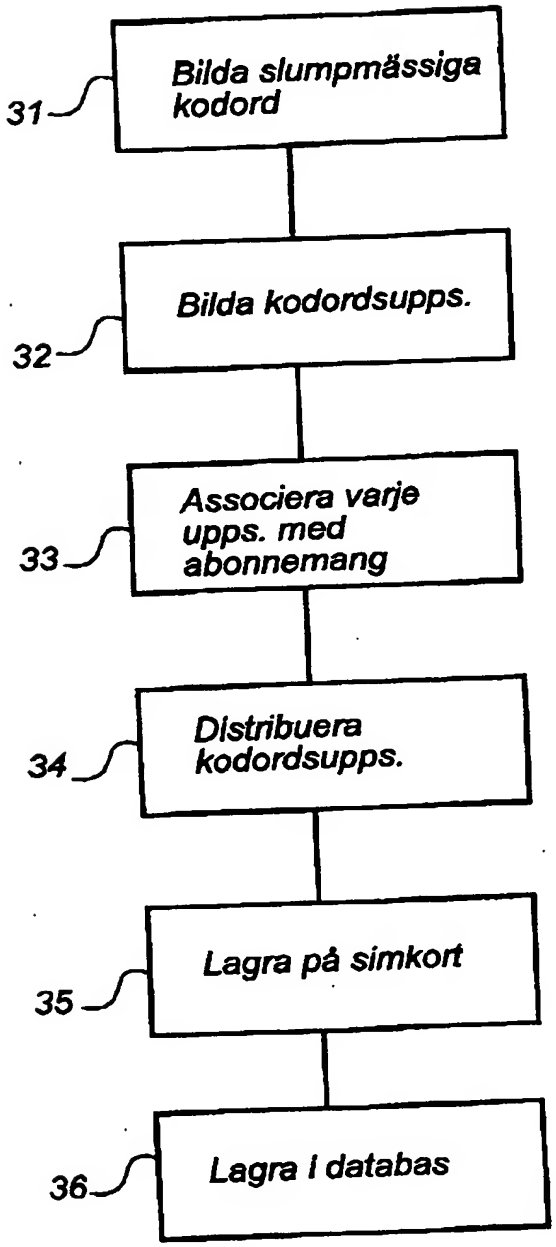

Fig 4

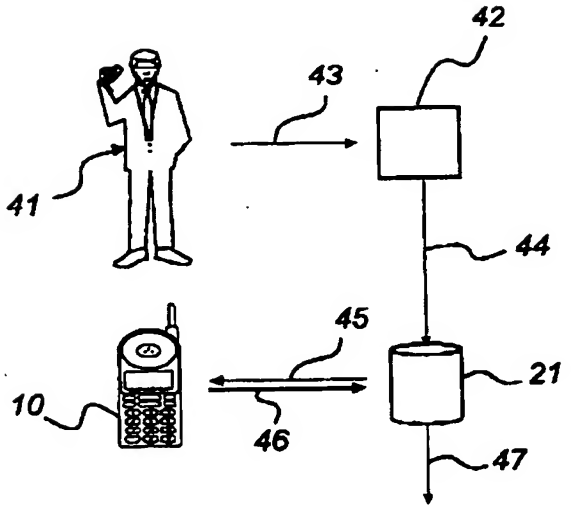

Fig 5a

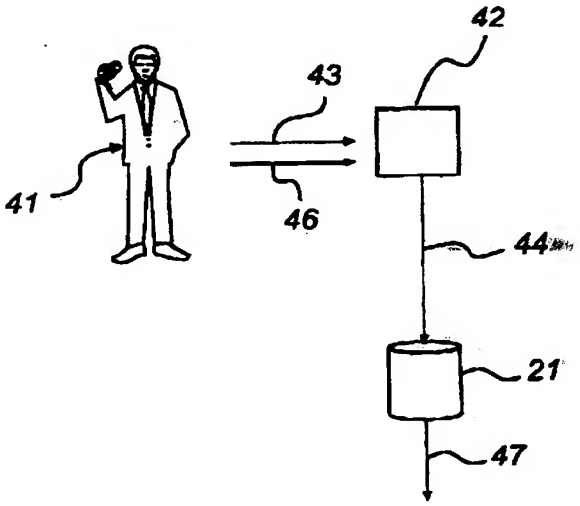

Fig 5b

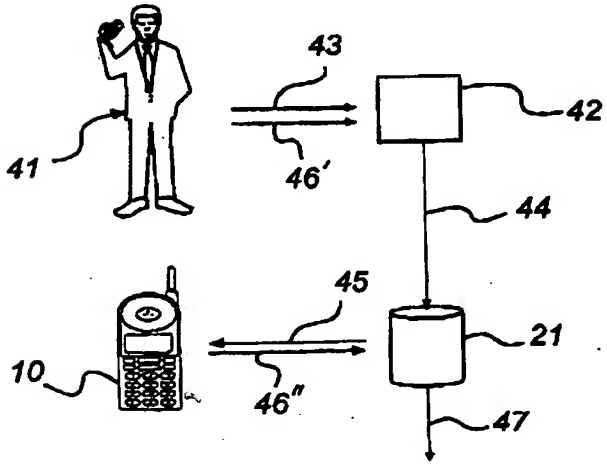

Fig 5c

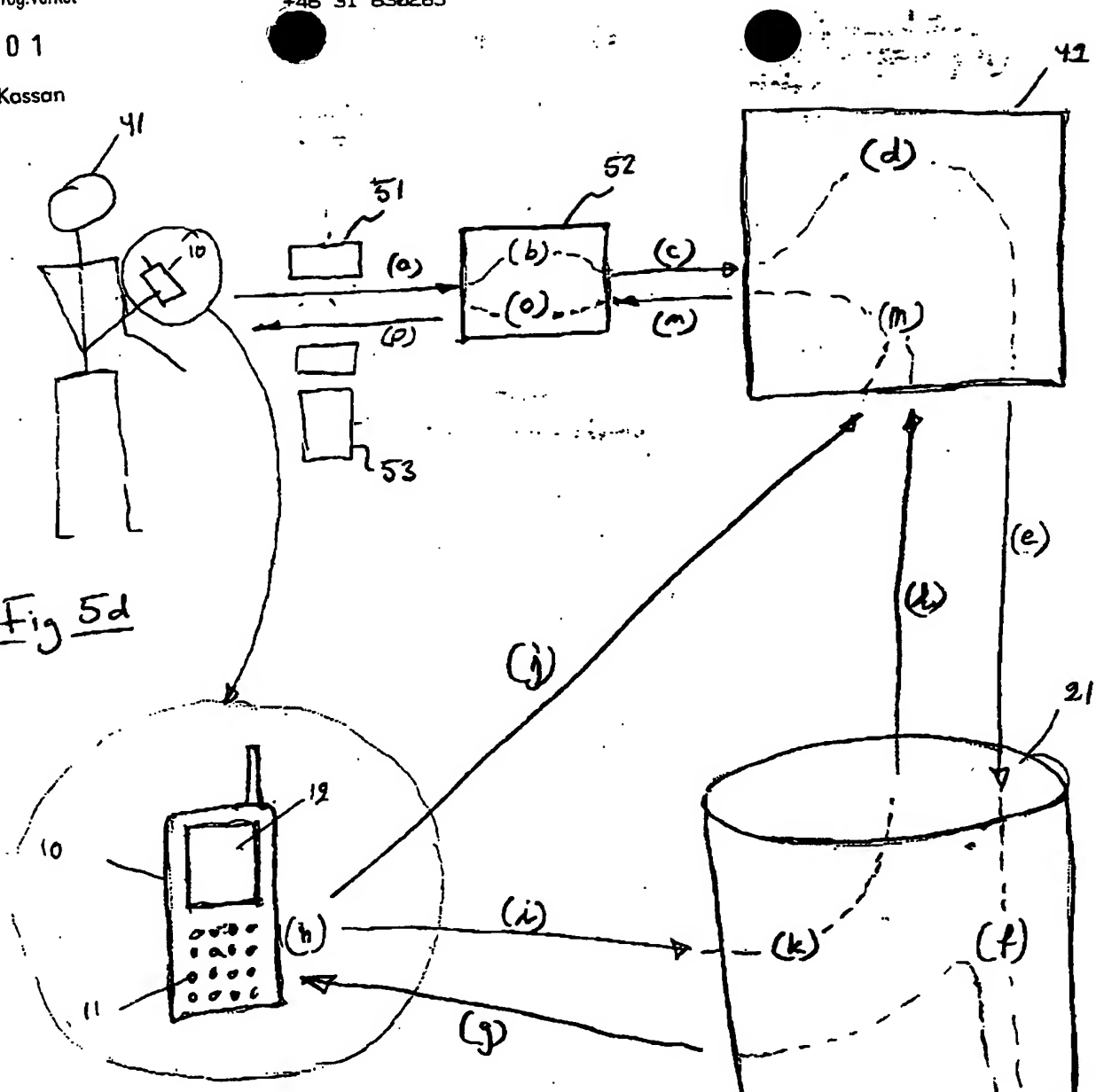

Fig 5d

Kodord i mobil och i ID-databas innan det aktuella uppdraget påbörjats:

- - -	1
- - -	
- - -	2
~~937119~~	
~~091702~~	
~~009270~~	
576362	
805209	
76 3268	
~~89~~ 1957	

Fig 1b